INTEL OPTIMIZED CASE STUDY SERIES

BeeKeeperAI Secures AI Algorithms with Infrastructure from Intel, Microsoft, and Fortanix

RESEARCH BY:

Matthew Marden

Mario Morales

Artificial intelligence (AI) requires large amounts of data from a wide variety of sources to optimize algorithm performance. This is an acute challenge for healthcare AI algorithms due to the generalizability standard required by many regulatory bodies. One of the greatest barriers to achieving better results from AI models is the difficulty in gaining access to sufficient amounts of diverse data. Due to regulations and compliance barriers, hospitals and health systems (e.g., data stewards) are hesitant to share their data due to growing privacy and security concerns and the vital need to protect patient information for both legal and privacy reasons.

To address this challenge, the Center for Digital Health Innovation at the University of California, San Francisco (UCSF) joined forces with Intel, Fortanix, and Microsoft to create an environment to allow algorithm developers and data stewards to securely collaborate. As a result of this successful collaboration, a new company called BeeKeeperAI was formed and spun out of UCSF to commercialize this technology.

Improving Healthcare Outcomes with AI

Healthcare AI algorithms are forecasted to improve healthcare outcomes by 30% to 40% while cutting treatment costs as much as 50%. BeeKeeperAI accelerates the validation of algorithms by providing a “zero trust” environment reducing the development time from years to months resulting in increased speed to market for healthcare AI. The platform also enables workflows for more efficient access to protected data, transformation, and orchestration across multiple data providers.

By leveraging the hardware-enhanced security of Intel Software Guard Extensions (SGX), the platform safeguards both the intellectual property of the algorithm model and the privacy of the healthcare data. In addition, the platform utilizes Fortanix's Confidential Computing Manager running in Microsoft Azure to safeguard the collaboration activities between the algorithm developer and data steward.

Algorithm developers who currently spend millions of dollars per model and invest years in securing the data can now greatly reduce the time to get their innovation to market.

BeeKeeperAI allows algorithm developers to submit an encrypted, containerized AI model via Azure to the data steward's HIPAA compliant Azure environment where the model and the data meet within the SGX secure enclave for validation of model inference. The Fortanix software stack manages keys and workflow to submit the encrypted container to the Intel SGX enclave on Azure. Throughout the process, the data is never moved, exposed, or shared, and the data steward can never see the algorithm inside the container. Upon completion of the validation process the algorithm developer receives a validation report, which provides statistics on the algorithm's performance. These high-level statistics do not infer anything about the data on which the algorithm was validated.

Work began on the platform when the Center for Digital Health Innovation (CDHI) could not access sufficient data to create AI algorithms that were generalizable. Mary Beth Chalk, Co-Founder and Chief Commercial Officer at BeeKeeperAI explained: *"Typically, you anticipate that an AI algorithm developed on a single institution's data would likely only perform well at that institution because it had not been developed with consideration of other factors such as different types of equipment, clinical workflows, or patient types."*

To address this challenge, the CDHI began working with Intel, which had invested in Fortanix's confidential computing platform. *"BeeKeeperAI's Chief Scientific Officer is a former Intel employee and through his connections we were introduced to the team at Fortanix,"* Chalk said. *"When we began to make the connections, we immediately saw how Fortanix's confidential computing environment could help to address the data access challenge for healthcare AI. Intel continues to be an incredible partner for us,"* Chalk says.

> **"Now we are able to help AI algorithm developers find the data stewards they need to validate their models."**
>
> Mary Beth Chalk,
> Co-Founder and
> Chief Commercial
> Officer,
> BeeKeeperAI

Faster, More Cost-Effective Development

With the capabilities of Intel, Fortanix, and Microsoft, Chalk and her eight-person staff were able to complete development of the minimum viable platform in June of 2021 (within 12 months). *"A month after its release we began working with large institutional customers who have a number of models they need to validate quickly,"* Chalk says.

Chalk spoke to the extent to which the technologies underlying the BeeKeeperAI platform have enabled efficient development and deployment for real-world use: *"Without Fortanix's confidential computing platform and Intel's SGX/Ice Lake environment it would have likely required two to three years to develop an end-to-end zero trust environment and triple or quadruple our staff,"* Chalk says. *"We would have spent our time and capital becoming a confidential computing* *company and not a secure healthcare AI collaboration platform dedicated to enabling the acceleration of medical breakthroughs that save lives, improve outcomes, and reduce the cost of care."*

BeeKeeperAI is already driving potentially transformative healthcare and clinical innovation. Chalk explained: *"Now we are able to help AI algorithm developers find the data stewards they need to validate their models."*

According to Chalk, algorithm developers who currently spend millions of dollars per model and invest years in securing the data can now greatly reduce the time to get their innovation to market. Given algorithm use in the development of innovative new treatments, this time savings can be hugely impactful. *"We're anticipating a 12-month reduction in time for novel healthcare AI, which was previously stalled due to the challenge of accessing sufficient data,"* Chalk says.

The Centrality of Zero Trust

Chalk also stressed the centrality of zero trust security in encouraging use by both algorithm developers and data stewards and linked this to the immediate uptake of the BeeKeeperAI platform. She noted that, with its hardware-based memory encryption, Intel SGX helps to isolate specific application code and data in memory. This means the BeeKeeperAI platform can use private regions of memory, known as Trusted Execution Environments, to increase the security of application code and data. With this safeguard, other organizations can confidently work together to validate the algorithms while protecting their intellectual property and keeping each organization's data confidential.

"With SGX nothing is seen end-to-end by any entity, and this accelerates our sales cycle," Chalk says. *"Without this promise of zero trust it would likely take us a minimum of 18 months to convince a CIO and CSO at an academic medical center that we would protect their data. The sales cycle would go from the current 180 days to 18 months overnight."*

In terms of the data steward infrastructure, BeeKeeperAI runs in their secure and compliant cloud-based environment. *"This has the attraction of leaving the data in their control at all times,"* Chalk says. BeeKeeperAI charges a Platform-as-a-Service license fee for platform access and uses a revenue-share model to compensate the data stewards. *"This may likely reduce the cost for the algorithm developers and allow them to get their models to market quicker because they have access to the data required to complete their regulatory approval processes faster and more efficiently,"* Chalk says.

In June 2021, BeeKeeperAI had two models go into two different secure enclaves and operate on two different sets of data, one at UCSF and one at UC Davis. *"The models ran on the data but couldn't see the data, UCSF and UC Davis couldn't see the model, and the BeeKeeperAI platform couldn't see either the data or the model,"* Chalk says.

Message from the Sponsor

Sponsored by Intel. Information based on internal estimates of BeeKeeperAI. Your results may vary.

See ways our partners are utilizing Intel products to benefit your business, visit the **Intel Solutions Marketplace.**

To learn more, click here

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

@idc @idc idc.com